PSWN

Public Safety Wireless Network

Security Field Data Collection and Analysis Report

Site #2
Digital Trunked Radio System

Final

July 1999

FOREWORD

This report presented by the Public Safety Wireless Network (PSWN) program documents security issues and candidate recommendations identified during the second of a series of security field data collection and analysis efforts. The primary goals of these efforts and the resulting reports are to raise security awareness and understanding and to help mitigate security risks associated with evolving public safety communications systems.

Questions or comments regarding the information contained in this document should be forwarded to the PSWN Program Management Office (PMO) at 800-565-PSWN. For additional information regarding the purpose and goals of the PSWN program, see the PSWN web site at www.pswn.gov.

TABLE OF CONTENTS

1.

1. INTRODUCTION

The Public Safety Wireless Network (PSWN) program has deployed case study teams to conduct detailed interviews with managers and users of public safety radio systems in selected regions of the United States. The case study interview guides used by these teams include several security-related questions. The PSWN program also has initiated a number of security-focused data collection and analysis activities. These data collection activities build on the security information gathered through the case studies by collecting more detailed security information at a few selected sites. A *Security Field Data Collection Summary Report* will be prepared at the conclusion of the initial series of security-focused data collection efforts. These efforts support the larger goal of establishing the PSWN program as a valuable information resource and a source of guidance for many aspects of public safety communications.

Under the security data collection and analysis effort, a first site visit was conducted at an Emergency Communications Center serving police, fire, and emergency medical services on October 8, 1997. The first site is the control center for an analog trunked system. The results of the first site visit are documented in the *Security Field Data Collection and Analysis Report Site #1 – Analog Trunked Radio System*.

A second site visit was conducted from November 9 through 13, 1998, at a Network Control Center (NCC) for a digital trunked radio system serving state and local public safety agencies. In addition to the NCC, a zone controller site, a remote radio site, and a dispatch center were visited in the course of gathering data about the system. This report documents the results of those efforts. All references to the agency visited have been removed from the report.

When conducting a site visit, the PSWN team uses an internally prepared security data collection plan as a guide to ensure all pertinent information is collected. This plan is included as Appendix B of this report. Site visits provide the PSWN team an opportunity to improve the plan based on lessons learned following each visit. This process ensures the PSWN team requests the latest, most accurate, security relevant information at subsequent site visits.

1.1 Purpose

The security field data collection activities will increase understanding of the emerging security issues associated with evolving public safety communications infrastructures. These efforts will provide insight into not only the risks associated with the computerization and digitization of those infrastructures, but also the security concerns and needs of the public safety community. In addition, the studies will identify best security practices and measures taken to decrease the risk to public safety radio components and information.

Security field data collection activities support the following goals:

- Identifying the criticality and sensitivity levels of data communicated
- Documenting communications infrastructures used, including wireless and wireline connectivities
- Describing existing technical and procedural security controls
- Identifying security concerns, as well as the frequency and nature of known security issues and incidents
- Capturing existing best security practices and security measures.

Additional security issues, concerns, and practices will be documented as data are collected at additional public safety agency sites. Those findings, along with the findings in this report, may reveal patterns or commonalities in the security of public safety communications. Dissemination of security issues, best practices, and candidate recommendations to the public safety community should provide valuable guidance as the community makes decisions about the security of its systems.

1.2 Scope

The security-focused field data collection is intended to gather security-related data on public safety communications infrastructures to enhance the understanding of possible risks to these infrastructures. This report is not an evaluation of the security practices of any particular public safety agency or of public safety communications infrastructures in general. Candidate recommendations are included for each security issue identified in the report. These recommendations and new candidate recommendations will continue to be evaluated during subsequent data collection activities for potential inclusion in a summary report.

1.3 Document Organization

This document is divided into the following sections:

- Section 1, Introduction—presents background, purpose, scope, and document layout.
- Section 2, Approach—describes the approach used in conducting the security field data collection and analysis.
- Section 3, System Description—presents a description of the system analyzed and the organization visited.
- Section 4, System Security Findings—presents issues identified during the data collection effort and any best practices used by the subject organization to secure its system.
- Section 5, Summary—provides a synopsis of the findings discussed in the previous section.

- Appendix A, Acronyms—contains a list of acronyms used in this report.
- Appendix B, Security Field Data Collection Plan—includes the data collection approach and detailed interview guide questions used during the site interviews.

2.

APPROACH

A four-step process was used to perform this security field data collection effort. The steps for this approach are described below.

Step 1: Coordinate and prepare for data collection effort

- Send the data collection plan for pre-data collection
- Identify personnel for conducting the security data collection effort
- Coordinate the data collection schedule
- Determine which site personnel should be interviewed
- Identify the type of system components at the site for pre-interview research.

Step 2: Collect system and site data

- Validate system information collected in Step 1
- Collect more detailed information about the site's system configuration, including a system diagram if possible
- Identify current security practices, concerns, and needs.

Step 3: Research and clarify data gathered from the site

- Collect data from various sources (e.g., Internet, professional journals) concerning security issues and concerns raised
- Recontact site personnel, if necessary, to clarify information gathered.

Step 4: Analyze and document security issues, candidate recommendations, and best practices

- Describe the security issues raised during data collection
- Provide candidate countermeasure recommendations, as applicable, for security issues
- Document existing best practices at the site
- Consolidate the site data and their analysis into a report.

3.

SYSTEM DESCRIPTION

The NCC visited under this effort is responsible for the management and control of a digital trunked radio system that is serving state and local public safety agencies. Figure 1 provides an overview of the system and its connectivity. The following subsections describe various aspects of the system.

3.1 General

The statewide implementation of the communications system includes construction of new communication towers around the state. Currently, the communications system is operating in Phase 1 of four phases, which covers approximately one-fifth of the state's geographic area. The communications system supports 1,000 trunked channels and 134 frequency pairs for local, district, and statewide communications. At present, the system supports only voice communications; however, if a cost effective trunked data solution becomes available in later versions of the current protocol, the agency will consider using it to transmit data on the system.

The state agency that owns the system has sole and exclusive responsibility for the selection of equipment, operation, management, and maintenance of the system and its services. The state agency staffs the NCC 24 hours a day, 7 days a week to assist user agencies and to support troubleshooting of the communications system.

3.2 System Connectivity and Management

The communications system has integrated communications controllers at the site, zone, and wide area levels. The NCC is connected to the trunked communications system by digital DS1 circuits. The digital microwave system connects all other sites into a system and uses 6 GHz for high capacity links and 6 GHz and 18 GHz for low capacity links. The microwave radio paths provide reliability of equal or greater than 99.999% and have an outage time less than 5.25 minutes per year. Microwave hops 25 miles or longer uses space diversity protection to eliminate multipath fading. Each path has a fade margin value greater than 40 dB per hop. Elliptical waveguide and tunable connectors are used to connect the microwave radio system to the antennas.

For the trunked communications system, fault tolerance is provided for on both the wide area and local levels. The zone controller that manages the trunked system is equipped with redundant cards, power supplies, and hard drives for all functions. In addition, the system uses alternate paths to maintain wide area coverage when a single point of failure occurs. If an alternate path is unavailable due to multiple points of failure, communications are still locally available using the built-in site trunking mode. If the site trunking mode becomes unusable, then radio to radio communications is available in the "Fail Soft" mode (base stations revert to conventional repeaters) as a last resort.

NCC personnel and agency communications division staff control and manage the system. The on-duty NCC operator uses a network management system and an alarm monitoring system to configure, control, and monitor the radio sites and the communications system. Both the management and alarm systems are connected to the primary radio site via leased lines. In addition, there is dial-in access to the primary site to allow communications division staff and the vendor to configure and control the system remotely when required.

NCC personnel and agency communications division staff develop and maintain talkgroup templates used for programming user radios. The same personnel also control the system key required to program radios, ensuring that only approved changes are made to radio unit templates. Each radio has a unique electronic identification (ID) that is checked by the system each time a transmission is made to make sure only valid devices use the system. The NCC system can make a lost or stolen radio invalid which prohibits it from transmitting or receiving any communications. If a lost or stolen radio is unreachable (i.e., turned off), the system will continue to attempt to invalidate the radio until successful. Once a lost or stolen radio is recovered, it can again be made valid.

3.3 Dispatch Centers

Seven statewide dispatch centers and one local dispatch center per county are planned for the system. Dispatch centers will consist of both computer-aided dispatch (CAD) and non-CAD systems for the immediate future. There are two to ten dispatchers, depending on the location, per shift to operate the dispatch consoles. The dispatch centers have the capability to record any conversation for up to 20 minutes in duration.

3.4 Encryption Capabilities

All channels are able to transmit either clear or encrypted voice communications and encryption is provided for those agencies that require it for their communications. All trunked repeaters in the system can relay encrypted voice between units with minimum degradation of audio quality and no decrease in the coverage compared to the quality and coverage for clear voice. Approximately 20 percent of radios, currently available or planned, support encrypted communications. The encryption mechanism used is Federal Information Processing Standard (FIPS) 140-1 compliant and the system is intended to migrate to be compliant with the Telecommunications Industry Association/Electronics Industry Association (TIA/EIA)-102 (Project 25) standards.

3.5

Physical Access to System Components

Physical access to all radio sites is restricted to authorized personnel. Fencing with locked gates is installed around the site perimeters. Entrance doors into the buildings that house communications and support equipment are locked at all times. Uninterruptible power supplies and generator backup power are provided at all radio sites. The site buildings were constructed with solid concrete and fire proof material on the walls and ceilings. Additionally, each site has entry, heat, and smoke alarms that send a notification to NCC personnel.

During normal working hours, a receptionist at the main entrance controls access to the building that houses the NCC. The entrance and exit to the parking lot, the main entrance to the building, and access to the floors within the building are controlled by swipe card devices during nonworking hours. At the time of the site visit, swipe card access was used only at two side entrances and one interior door of the building during normal working hours.

Since there are only 200 people located in the building, the agency determined that there is no need for a physical security officer to be assigned to the building. However, a security officer from the state agency headquarters performs security duties such as issuing swipe cards and keys as needed.

4. SYSTEM SECURITY FINDINGS

This section describes the security issues and the best practices identified during the site visit and as a result of subsequent follow on discussions with site personnel.

4.1 Security Issues

The security issues described in this section include possible implications or associated risks along with candidate recommendations on mitigating the risks. Table 1 summarizes the identified security issues and the corresponding recommendations. The following subsections provide more details.

Table 1
Summary of Security Issues and Candidate Recommendations

Section	Security Issue	Candidate Recommendation
4.1.1	Physical security at the NCC and a dispatch center is relatively weak.	The main entrance to the building housing the NCC should be swipe card activated at all times. Swipe card controls on the interior stairwell doors should be activated at all times. Lock doors providing access to NCC, or install and activate swipe card readers for those doors.
4.1.2	Dial-in modems at the primary site could be exploited.	Network managers should be made aware of network dial-in vulnerabilities and security practices (e.g., modem dial-back, token-based authentication, password parameter settings). Security policies should address this remote management and maintenance point of entry.
4.1.3	No comprehensive contingency or disaster recovery plan exists.	Develop comprehensive contingency/disaster recovery plans that address operational procedures to be followed by dispatchers, radio users, and management. The contingency plans should be tested periodically based on the criticality of operations.
4.1.4	No consolidated security policy or procedures exist.	Develop agency security policy and procedures applicable to the communications system and make them available to personnel responsible for implementing, operating, and maintaining the communications system.
4.1.5	Communications system data maintained on the agency's LAN is not adequately controlled.	Restrict access to the communications system data maintained on the agency's LAN to only those personnel that require access to the data to perform their mission.

4.1.1 Physical Security at the NCC and a Dispatch Center Is Relatively Weak

The building that houses the NCC is accessed by entering a fenced and gated parking lot and then entering the building's main entrance door or one of two side entrance doors. Both the entrance and exit gates to the parking lot and all three exterior building entrance doors are swipe card enabled. However, during normal working hours, the parking lot gates are left open and the main entrance “visitor door” does not require use of a swipe card to enter the building. There is a receptionist at the main entrance to the building during these hours; however, on two occasions during the site visit, the receptionist was not present when the building was entered. The interior stairwell entrances to each floor and the elevator keypad are also swipe card enabled. However, at the time of the site visit, the interior stairwell doors were all keyed to be open during normal business hours. Only one interior door of the building was swipe card activated during normal business hours.

The third floor of the building houses the communications division and other staff of the public safety agency. The NCC is located on this floor and has doors on two hallways. Both hallway doors are not locked and are typically left open. The combination of the third floor and building access controls, or lack thereof, implies that a person with everyday access to the building could easily gain access to the third floor and the NCC. In addition, anyone could gain access to the building and then to the third floor and the NCC with little trouble.

Access to a dispatch center was also poorly controlled. The building that houses the dispatch center is accessed by entering either an “open” parking area outside the fenced compound and then walking inside the compound, or entering a fenced and gated parking lot within the compound and then entering the building. At the parking lot entrance is a guard booth with swipe card reader and a wooden, raisable entrance arm. However, the guard booth was not manned during the site visit and anyone could either walk around the raisable entrance arm or break it by driving through the arm. The building entrance was not locked.

The dispatch center was located one floor above the building entrance. Entrance to the dispatch center itself was controlled by personnel within the dispatch center. Visual recognition or presentation of an appropriate employee badge and visit coordination was required. Further, it was noted that the dispatch center had a video monitor which, on a rotating basis, displayed the parking lot area, the gate entrance, the building entrance door, and a guard station in another building that controlled access through the gate. However, only one desk at the dispatch center had a clear view of the monitor displaying the entrances. It was stated during the site visit that as late as 11:00 p.m. the building entrance was unlocked.

Candidate Recommendation:

Ideally, the building housing the NCC should have its main entrance controlled to allow only authorized visitors and personnel into the building. Activating the swipe cards on the parking lot during normal business hours would probably be a significant inconvenience to authorized personnel. It would seem a reasonable compromise to have the main entrance swipe card activated at all times with the receptionist having the capability to allow entrance to the facility, as required. Access within the building and to the NCC should also be controlled. Activating the swipe card controls on the interior doors, assuming that all authorized building tenants would be authorized access to all floors, would ensure that only building occupants could gain access to a floor. In addition, either the NCC should have its doors locked during normal business hours, or swipe card readers should be installed that allow only authorized staff access to the NCC.

The dispatch center building should have swipe card access capability on the exterior door of the building, or if that is not practical, an interior door installed with swipe card access capability that leads to the dispatch center floor. Consideration should also be given to enabling a swipe card capability on the fence gate at the entrance to the interior parking lot instead of the raisable entrance arm.

During a conversation with the public safety agency that occurred after the site visit, it was discovered that the interior doors of the building housing the NCC had recently been swipe card enabled. This has the effect of minimizing the opportunity for an outsider to gain entrance to the building and then immediately have access to all floors within the building. Any outsider would be restricted to the lobby area until escorted or until provided with a badge allowing freedom of movement within the building.

4.1.2 Dial-in Modems at the Primary Site Could Be Exploited

The primary site has two dial-in modems that are used for remote administration or monitoring of the radio system. One modem is used to configure the radio system controllers and to perform maintenance and updates of the radio system software. Connection to the system is controlled by user identification (ID) and password with additional passwords needed to access certain parts of the system. The other modem is used to access the alarm and control system that monitors many different facets of the telecommunications backbone and the physical environment of the remote sites. Connection to this system is also controlled by user ID and password. These two modems introduce an avenue into the system that could be used to modify or compromise many aspects of the radio system. The passwords used for allowing or denying access to the system are not currently configured to be difficult for an attacker to determine. In addition, there is no method used to limit who or what can connect to the modems.

By allowing connections and access attempts to anyone with a modem, commonly used automated tools called wardialers could exploit these points of entry. Wardialers are used to identify modems among a range of phone numbers. They may be configured to repeatedly attempt to login to a remote computer once a modem connection is made, using numerous user IDs and a dictionary of possible passwords. It is possible to configure wardialers to respond with passwords constructed in accordance with various configuration parameters. Once an attacker has connected to the radio system, a talkgroup could have its name or membership modified, and the whole system could be shut down or made unusable by a determined attacker. Likewise, the potential exists for the alarm system to have its operation maliciously modified or disabled.

Candidate Recommendation:

Awareness of the potential vulnerabilities associated with remote access capabilities should be raised in the public safety community because it is likely that similar configurations exist on other public safety communications networks. Security safeguard options should be considered by network managers to mitigate the risk of such vulnerabilities. Options include modems that disconnect and then dial a pre-configured number, authentication mechanisms that require the user to possess a physical device as well as a password, and configuring the password to be difficult to guess but easy to remember (e.g., j0e4*lite—joe for starlight).

4.1.3 No Comprehensive Contingency or Disaster Recovery Plan Exists

The system management staff is aware of the importance of contingency plans and has been working on the development of such plans. However, there are no documented contingency plans. Contingency plans should address detailed step-by-step actions to be taken in emergency situations such as when a dispatch center is unavailable, or users are unable to communicate using the wide area communications system. Without documented contingency/disaster recovery plans, individuals may be unaware of their roles and responsibilities under emergency conditions.

Candidate Recommendation:

Develop comprehensive contingency/disaster recovery plans that address operational procedures to be followed in an emergency situation that affects the communications infrastructure (e.g., fire at a site, earthquake, storm, and system failure) by dispatchers, radio users, and management. These plans should be available to dispatch centers and all users with responsibilities identified within the plans. The plans should also address how to resume normal operations after the emergency situation has passed.

The contingency plans should be exercised periodically based on the criticality of operations so there can be reasonable assuredness of a continuity of essential operations in the event of a disaster or emergency. The following table presents the frequency with which certain portions of the contingency plans should be exercised.

Criticality Level		Description	Frequency
1	Critical	• Can only be done by the radio system. • No alternate processing capability exists.	Quarterly
2	Essential	• Alternate methods available and would be implemented until the radio system is restored.	Bi-annually
3	Important	• No radio system is needed. • Other methods are available.	Annually
4	Non-Critical	• Can be delayed until a damaged system is restored and/or new equipment is purchased.	As needed

4.1.4

No Consolidated Security Policy or Procedures Exist

No consolidated set of security policies or procedures applicable to the agency's communications system exists. A security policy should describe how an organization manages and protects a system and information about the system. Security procedures should provide users and managers with specific instructions on how to securely interact with a system. Although a number of high level security policies have been developed as called for in the system's Request for Proposal, there is no single document or repository for security information about the system. This makes it difficult for the agency to determine the overall system security posture and for the agency personnel responsible for security to identify how security should be managed.

In addition, the lack of a security policy can lead to an unsecurely configured system and to users not following good security practices. For example, during the site visit it was discovered that users were essentially sharing a user ID and password by leaving a number of systems in the NCC logged in continuously. In effect, shift changes occur with the outgoing user not logging out and the incoming user not logging in but using the system from the time they arrive on shift. In addition, no screen savers are used on the NCC's systems that would require a user to present a password to activate the terminal after a period of inactivity, and users are not required to log out when leaving a system unmonitored for a period of time (e.g., to take a break or coordinate with someone in another office). With the already identified weaknesses in the physical security of the NCC, it would be relatively easy for someone to enter the NCC during such a time and modify system parameters to adversely affect the system.

Candidate Recommendation:

Develop agency security policies and procedures applicable to the communications system and make them available to personnel responsible for implementing, operating, and maintaining the communications system. The security policy should enforce security requirements set forth in federal radio communications regulations and directives (e.g., user ID and password should not be shared, passwords should be not easily guessable).

4.1.5 Communications System Data Maintained on the Agency's Local Area Network Is Not Adequately Controlled

The public safety agency maintains information about its communications system on the agency's local area network (LAN). This information includes template files, job tickets, network databases, and system drawings. The information is used to assemble billing information for users of the system, to prepare statistical data about the system, and to provide an easy method of retrieving data about the system for management and administrative use. Currently anyone in the communications division is able to access and modify the communications information on the LAN. Billing personnel have only read access to the data.

Although the system data on the LAN is not used to control the communications system, access to it should be controlled. The information on the LAN provides a great deal of critical information concerning the communications system and its operation that could be useful to someone interested in disabling or manipulating the system. Only communications division personnel that require access to the communications system data in performance of their duties should be allowed access to it.

Candidate Recommendation:

Restrict access to the communications system data maintained on the agency's LAN to only those personnel within the communications division that require access to the data to perform their mission. The access control mechanism on the LAN could be used to limit the rights that users or groups of users have to the communications system data. For example, some users could be granted read access while others are granted read and write access based on their operational duties.

4.2 Best Security Practices

The "best security practices" identified during the site visit and presented in this section include concepts, designs, and procedures that appear to be reasonable methods of mitigating security risks to public safety communications infrastructures.

4.2.1 System Has Strict Configuration Management

Originally the vendor preprogrammed all talkgroups into all radios; however, this process allowed any entity with the appropriate software to activate any talkgroup in their radio even though they were not included within the talkgroup's functional or operational chain. In addition, the same software allows certain features to be activated that could cause unwanted effects on the system. Therefore, the communications division reprogrammed all the radios to contain only the talkgroups needed by the organization owning the radio. In addition, the communications division has maintained rigid control of the system's "control key" that allows certain features and functions to be activated, including adding talkgroups to a radio.

By actively controlling talkgroups programmed into the radios and restricting the features and functions that organizations can activate, the communications division ensures safe and efficient operation of the system. All changes made to radio talkgroup templates or the network database are documented by the requestor, reviewed by the engineering group, and must be approved by communications division management before implementation. User organizations are made aware of the strict configuration management control exercised by the system owner via a user agreement that the system owner and user organization must sign prior to the user organization being included in the system.

4.2.2 Data Is Backed Up Regularly

At the NCC, systems that are integral to controlling and monitoring the communications system are backed up weekly or more frequently if there is greater activity in the databases and information that is used by the systems. In addition, information stored on the LAN concerning the communications system is backed up daily as part of the LAN backup process. This information includes template files, job tickets, network databases, and system drawings. The backup media are stored at off-site facilities after the data is backed up. This practice allows the NCC to restore data in a timely manner if it is lost due to system malfunction.

4.2.3 Alarm and Control Monitoring Occurs at Antennae Sites

The communications system has alarm and control monitoring for the trunking equipment, telecommunications backbone equipment, the equipment shelters, and antennae towers. The antennae site perimeters are surrounded by barbed-wire fences and locked gates to dissuade unauthorized persons from gaining access. Only limited personnel have keys for the locked gates. Access to the shelters activates an alarm that is broadcast to multiple locations (primary location being the NCC) where action is taken to validate the alarm, including sending personnel to investigate if the reason for the alarm is undeterminable. The information recorded by the system includes site identity, time of the event, and any other pertinent data concerning the event.

4.2.4 Adequate Environmental Controls Are in Place

The antennae sites have adequate environmental controls installed and operational. These controls are:

- Fire extinguishers at each exit door
- Heat and smoke detectors
- Uninterruptible power supplies
- Emergency power provided by auxiliary generators with fuel to operate for extended periods
- Fuel tanks provided with low fuel indicators tied into the alarm system
- Emergency switch and emergency shutdown procedures
- Grounding to protect the sites against lightning hits.

4.2.5 Self-Contained Maintenance Capability Exists

The agency operates its own maintenance facility, which provides limited component repair and programs the features, functions, and talkgroup templates into radios. Talkgroup template construction, including feature configuration, is performed by Communications Division staff associated with the NCC.

The agency has exclusive responsibility for operation, management, and maintenance of the radio equipment, including features and functions. The NCC personnel handle requests for radio repair by coordinating transportation of the radios to the maintenance facility. Non-state and other agency mobile radios are maintained by commercial companies. Those companies can do limited component repair and are not permitted to reprogram radio functions or features. Only the agency's radio technicians are able to reprogram the radios and then only with the consent of the NCC personnel and a valid job ticket authorizing the reprogramming. In addition, if a radio must be shipped to the manufacturer for repair, the internal programming is deleted before shipment, ensuring programming control and system information is maintained by the system owner.

4.2.6 Communications Are Not Readily Available to Unauthorized Personnel

Conventional analog communications have long been able to be monitored by the public through the use of radio scanners. Over the past few years, a new generation of trunking scanners has enabled the public to easily monitor trunked analog communications. Both trunked and conventional digital communications may be monitored; however, with current scanning capabilities, the information that is monitored sounds like a series of noises to the human ear. The information is understandable only after another radio within the communications system has "undigitized" the information.

The agency has had requests from outside commercial agencies (e.g., towing companies) to be included in their network so they can monitor transmissions. The agency neither has included these agencies in their network nor has any intention of doing so in the future. The agency also indicated that they had heard of commercial scanner manufacturers requesting digital translation information from radio system manufacturers with the likely intent to produce a scanner capable of monitoring, in an understandable manner, digital trunked radio communications. Additional steps taken by this agency are keeping the control key used for programming radios under their direct control and not allowing wildcard IDs to affiliate with the communications system. Even with these types of precautions, the agency should be aware that it is only a matter of time until a scanner is developed that will allow the public to easily monitor and understand trunked digital radio communications. At that point, only the use of encryption will ensure a high degree of voice communications confidentiality.

5.

SUMMARY

The security issues identified during the second site visit and through subsequent information gathering are documented in Section 4 and are summarized as follows:

- Physical security at the NCC and a dispatch center is relatively weak
- Dial-in modems at the primary site could be exploited
- No comprehensive contingency or disaster recovery plan exists
- No consolidated security policy or procedures exist
- Communications system data maintained on the agency's LAN is not adequately controlled.

The security issues identified are related to physical, communications, and administrative and management security. Controlling access to the facility or dispatch center is one way to easily provide a first level of protection to the system management components. Dial-in access to the system, which is not under the control of the owning agency, increases the risk of unauthorized personnel accessing the system and should not be allowed. Developing and exercising plans, procedures, and policies that specify security processes and provide detailed guidance to agency staff will reinforce the need for security to agency staff and help identify areas in which security can be improved. Limiting access to information about the communications system to the minimum amount of people limits the opportunity for both inadvertent and intentional disclosure of such information.

APPENDIX A

ACRONYMS

APCO	Association of Public Safety Communications Officials
CAD	Computer-Aided Dispatch
FIPS	Federal Information Processing Standard
ID	Identification
LAN	Local Area Network
MHz	Megahertz
NCC	Network Control Center
PMO	Program Management Office
PSWN	Public Safety Wireless Network
TIA/EIA	Telecommunications Industry Association/Electronics Industry Association

APPENDIX B

SECURITY FIELD DATA COLLECTION PLAN

DRAFT—Do Not Quote or Cite

Security Field Data Collection Plan

1.0 INTRODUCTION

A series of security field data collection and analysis efforts is being conducted with the primary goals of identifying security issues and concerns associated with evolving digital land mobile radio (DLMR) systems. This *Security Field Data Collection Plan* was developed to ensure consistency and adequate coverage across the organizations at which data is being collected.

2.0 APPROACH

The following steps outline the high level approach used in conducting each security field data collection and analysis effort.

Step 1: Coordinate and prepare for the data collection effort

- Identify personnel for conducting the security data collection effort
- Coordinate the data collection schedule with the organization
- Determine which organization personnel should be interviewed
- Identify the type of system components at the organization for pre-interview research
- Ask for documentation containing descriptions of the identified system components and system diagrams
- Provide the organization point of contact with the Security Field Data Collection Plan security questions and background information.

Step 2: Collect system and organization data

- Collect data by reviewing the documents and diagrams provided by the organization
- Visit the organization and interview personnel using the data collection plan interview guide
- Validate the collected data
- Tour facility and observe operating environment

- Collect additional system and security information
- Identify current security practices, concerns, and needs.

Step 3: Research and clarify data gathered from the organization

- Conduct research on security issues and concerns raised
- Recontact the organization, if necessary, to clarify information gathered.

Step 4: Analyze and document security issues, candidate recommendations, and best practices

- Describe the security issues raised during data collection
- Provide candidate countermeasure recommendations for security issues
- Document existing best practices at the organization
- Consolidate the organization data, analysis, and recommendations into a report.

3.0 SECURITY QUESTIONS

The security questions found on the following pages are categorized as follows:

- General
- Administrative security
- Physical security
- Automated information system (AIS) and network security
- Communications security
- Portable/mobile radios
- Portable/mobile data
- Other.

These questions serve as guidelines to the interviewer. It is expected that discussions will expand upon these questions. A glossary is provided at the end of this plan to help clarify terms used in the questions.

GENERAL

Agency/Organization:
Agency Contact:
Job Title/Function:
Telephone Number/Fax Number:

System operations:

- Number of users/radios
- Coverage (county, state)
- Types of users (police, fire, EMS, other)
- Number of dispatch centers/dispatch positions at each center
- Number of dispatchers per shift
- Number of channels and frequencies

Type of equipment used:

Manufacturer of radio system

Product name

Type of services:

- Encryption
- Voice and data capability
- Agencies using mobile data
- Paging capability

Sensitivity of voice/data stored, processed, or transmitted? (Confidentiality, Integrity requirements)

Mission criticality of operations? (Availability requirements)

May we obtain a high-level system diagram, even if hand drawn?

ADMINISTRATIVE MANAGEMENT

Security Policy

Does a written security plan exist for the RF network and any wireline networks or systems?

What kind of information does the security plan contain?

Who is responsible for reading and maintaining the security plan?

Does a written security policy exist for the organization?

If yes, does this policy cover AIS and radio systems?

If yes, is the policy consistently enforced?

If yes, may we obtain a copy of the written policy?

HHas any type of security evaluation or security testing been performed at the organization?
If yes, when was the last time an ST&E was conducted?

May we obtain a copy of the ST&E report?

Contingency Plans

ADMINISTRATIVE MANAGEMENT

Is there a contingency plan?

If yes, what is the scope of the contingency plan?

Is the contingency plan tested periodically and updated?

When was the last time the contingency plan was tested and updated?

Is there any redundancy available for consoles and communications connectivity?

Is the system capable of operating in a degraded state, if necessary? Please describe.

Is there a “ready-to-use” site designated in case of unavailability of the primary site?

Where is the “ready-to-use” site located?

Do contingency operations (i.e., emergency sites and equipment) provide the same level of security controls as regular operations?

Data Backup

Are the system/network data and resources backed up periodically?

- How often are they backed up? (Incremental backup/full backup)
- Is there an off-site storage facility for backup media?
- How often are the backup media sent to the off-site facility?

Configuration Management

Is there configuration management of computer programs?

Who is responsible for reviewing and approving any changes made?

Are all changes made to the system documented?

Security Training

ADMINISTRATIVE MANAGEMENT

Are users provided security training?

How often do they receive security training?

What subjects does the security training cover?

What methods are used to provide security training (e.g., sessions, memorandums)?

ADMINISTRATIVE MANAGMENT

Personnel Security

Is a personnel security policy established?

Is a background check required for users (e.g., employees, contractors) prior to gaining access to the system?

Is a background check required for cleaning and maintenance personnel prior to being hired?

Is there any additional or more detailed check required for administrators of the system?

Are contractors and support personnel (e.g., cleaning, vending, maintenance personnel) subject to the same check as users and/or administrators?

Maintenance/Services

Does the organization own the maintenance facilities?

Who performs equipment maintenance services?

What type of maintenance services are performed?

Are maintenance activities monitored to ensure security?

Is DLMR equipment transported to and from maintenance locations in a secure manner?

Is equipment tested after being serviced to ensure that security controls or functions have not been tampered with?

Are all maintenance activities recorded?

Is the maintenance record kept for a specified period of time?

PHYSICAL

Facility

Is a physical security officer designated in writing?

How are the facility perimeters protected?

Who has access to the communications system *facilities during duty hours?*

How is access to facilities controlled during duty hours?

Is there access control at the facility entry (guards/locks)?

Who has the building master keys for the facilities?

Are visitors logged in and out?

Are bags searched upon entry (even if random)?

Are bags searched upon exit (even if random)?

Are identification badges required for access?

Are visitors required to wear badges at all times?

Are visitors escorted at all times?

Is surveillance equipment used?

How is access to facilities controlled after duty hours?

Who has access to the facilities after duty hours?

Computer Room(s)

PHYSICAL

What computer room(s) exist to manage and support the organization’s communications?

- What are the functions of each?
- Where are they located?
- What type of computer equipment does each computer room house?

Who has access to the computer rooms?

How are the areas secured where computer equipment is stored?

Are doors locked at all times?

Are cipher locks used? If so, where/under what conditions?

If cipher locks are used, are the combinations changed regularly? When?

Are visitors logged in and out?

Are visitors escorted at all times?

Are computer rooms manned 24 hours a day, 7 days a week?

Dispatch Center

PHYSICAL

Who has access to the dispatch center?

What physical security measures (e.g., *guards,* keys, access cards) are used to prevent unauthorized access to the dispatch center?

Are doors locked at all times?

Are cipher locks used? If so, where/under what conditions?

If cipher locks are used, are the combinations changed regularly? When?

Are visitors logged in and out?

Are visitors escorted at all times?

Is surveillance equipment used?

Radio Sites

PHYSICAL

Who has access to the radio sites?

Are physical access control measures used to prevent unauthorized access to the sites' perimeters and shelters ?

Are the radio sites collocated with other agencies, contractors, or commercial organizations?

If yes, what are the physical security measures used to control the shared sites?

Do the sites comply with any physical security requirements set forth in the specified regulations (e.g., county jurisdiction code)?

Do physical access control devices activate alarms at a central location or local police department?

Are sites regularly inspected by authorized personnel?

Are the site locations published?

Are the heat and humidity alarms installed?

Telephone Closet

Who has access to the telephone closet?

Are doors locked at all times?

Are keys changed regularly? When?

Environmental

PHYSICAL

What environmental controls are in place to protect the system and the facility under emergency conditions?

- Are heat and smoke detectors installed in the ceilings and under raised floors?
- Is there a fire alarm?
- Is there a fire suppression system?
- Is the fire suppression system tested periodically?
- Is there a raised floor?
- Are there uninterruptible power supplies?
- Is there an emergency power capability?
- Is there a procedure to ensure that fuel running the auxiliary generators is sufficient and not contaminated?
- Is there an emergency switch and emergency shutdown procedures?
- Is the air conditioning system dedicated to the dispatch center or to the computer room?
- Is backup air conditioning available?
- Is proper grounding provided?
- Are the radio sites properly installed to protect against lightning?
- Is alternate routing available for power and phone services?

AIS/NETWORK (System/Network Administrators)

***** Note *****

This section addresses the questions for system/network administrators responsible for managing any wireline system or network that interfaces with the RF network.

Identification and Authentication

Are there procedures established to manage authorized user accounts on the system/network (e.g., create, delete, disable)?

How are user accounts/passwords distributed?

Identify any password constraints used by your system:

- Password length
- Password composition
- Password aging (How often must passwords be changed?)
- Password history (Are old passwords prohibited from reuse for a certain time period?)
- Change of initial password
- Resetting of forgotten passwords (Is a change then required?)
- User account locked out after a specified number of unsuccessful login attempts.

Are there procedures for handling accounts for users no longer requiring access to the system or network?

Is a list of user accounts maintained, reviewed, and updated? How often?

Access Control

Are there different levels of access to the system/network (e.g., users, system/network administrator, security administrator)?

What kind of privileges does each level have?

How are user’s access privileges to the system or its data determined?

Is there network-based remote access to the local area network (e.g., Internet, Intranet, WAN)?

AIS/NETWORK (System/Network Administrators)

Audit

Are audit trails available? (electronic logs of security related events performed by system users)

What kinds of security events are recorded in the audit trails?

Who reviews the audit trails? How often?

Are security activities on network hosts recorded? If so, who reviews? How often?

Remote Dial-in Access

Is there any dial-in access to the network? If so,

- Who has dial-in access to the system/network?
- To what components is dial-in access allowed?
- What functions are performed remotely?
- Are there any security controls for the remote access? (e.g., dial-back modem, strong authentication)
- Are there constraints for failed access attempts?
  - How many times is failed access allowed?
  - What occurs if the number of failed accesses is exceeded?

Is a list of user accounts for dial-in access maintained, reviewed, and updated? How often?

Other

Is any virus protection provided for the components that are a part of the system/network?

AIS/NETWORK (System Users)
***** Note ***** **This section addresses the questions for system users that access the system/network to perform their functions.**
Identification and Authentication

AIS/NETWORK (System Users)

Are you required to present your ID and password before you access the system/network?

Who assigns your ID and initial password?

Do you change your initial password at the first login?

How often do you change your password?

Are there policies or procedures for selecting passwords?

What is the minimum length of a password?

Are you required to select a combination of alphabetic and numeric characters for your password?

Does the system/network notify you of the need to change your password?

Are there procedures for reporting forgotten passwords?

If you forgot your password, who do you contact to receive your password?

- Is your password the same password you used or do you receive a default password?
- If you receive a default password, do you need to change the password immediately?

Are there procedures for reporting security incidents?

Do you know how many attempts you are allowed to enter your user ID or password before your account is disabled?

Are there procedures for reporting that your account is disabled?

Access Control

AIS/NETWORK (System Users)

What are your responsibilities for controlling access to information on the system?

Are you restricted to accessing only applications necessary for your job functions?

If not, what other applications are you able to access?

Is your terminal disconnected after an extended period of inactivity?

Do you log out when you leave your terminal unattended?

Remote Dial-in Access

Do you have dial-in access to the system?

What functions do you perform remotely?

Are you required to use your ID and password for dial-in access?

Who assigns your ID and password for dial-in access?

How often do you change your password ?

Other

Do you run anti-virus software regularly?

What would you do if you identified a virus on your system?

COMMUNICATIONS

Encryption

Is encryption provided to protect data transported among the system components?

What type of encryption is used?

Is encryption method documented and approved?

Is the control channel encrypted?

If no, do you have concerns about an unencrypted control channel being used to exploit radio communications?

In an emergency situation, how is sensitive information transmitted (via a clear channel or an encrypted channel)?

Key Management

Are written guidelines established for the handling and safeguarding of keying materials?

What is the key lifetime?

How are encryption keys changed?

How are key loaders protected?

How are radios with the current key loaded protected?

Are there procedures for protecting keys during their life cycle (e.g., generation, distribution, storage, destruction)?

When keys are compromised, are they destroyed in a secure manner?

Redundancy

Is an alternative communications path available in case a primary path fails?

Is there adequate backup (spare) communications equipment available?

Emission Security

When the system was designed, had emission security been considered?

Do you have concerns about electronic emissions being compromised and used to exploit the radio system?

RADIO (Portable/Mobile)

User Verification

Does the radio authenticate the currently assigned user?

Do the radio system components authenticate themselves to one another to ensure that only valid radios may be used?

What are the procedures for managing system users?

What are the procedures for managing talkgroups or channel assignments?

- Who assigns users to talkgroups?
- How are talkgroups assigned? by function?
- How are channels assigned? (by function?)

Encryption

Is encryption provided for radio equipment?

What percentage of mobiles and portables have data?

What type of encryption is used?

Is the encryption on the radio system transparent (e.g., uses end-to-end encryption)?

Are there policies and procedures to enforce the use of the encryption feature?

Do you use the encryption feature?

Do you turn this feature on and off?

Have you experienced any impact on operations due to the use of encryption (e.g., minimized range, degraded voice quality)?

Are multi-encryption modes implemented to meet an interoperable need?

Have you experienced any interoperability problems due to the use of incompatible encryption schemes between your system and others?

Have the cryptographic components used in the system been FIPS 140-1 certified?

If you don’t use encryption, what are the reasons that you don’t use it?

Over-the-Air-Rekeying

Do you currently use over-the-air-rekeying (OTAR)?

- If yes, how is OTAR managed?

- How many people are authorized to manage rekeying?

Remote Dial-in Access

Who has dial-in access?

To what components is dial-in access allowed?

What functions are performed remotely?

Are there any security controls for the remote access? (e.g., dial-back modem, strong authentication)

Are there constraints for failed access attempts?

How many times is failed access allowed?

What occurs if the number of failed accesses is exceeded?

Redundancy

Is any redundancy available for dispatch consoles and RF network connectivity?

Lost and Stolen Radio

What are the procedures for handling lost or stolen radios?

How is the loss reported to radio managers?

Is there a capability to disable such radios?

If such radios contain encryption capabilities, is any different action taken upon their loss than that taken for non-encryption capable radios?

Are procedures established for controlling access to MDTs and radios?

What are the procedures for activating radios recovered from being lost or stolen?

Are procedures in place for the secure disposal/destruction of radios?

Are procedures established for use of the emergency activation button?

Portable/Mobile Data

Portable/Mobile Data

Does your organization utilize data communications?

What type of MDTs, MDCs, laptops, or portable data terminals used?

Portable/Mobile Data

Property Disposal

Are procedures in place for the secure disposal/destruction of MDTs/MDCs?

Is all organization/operation’s specific data removed from the device?

For an MDT/MDC that is no longer used by the organization, is information that would allow continued access to the organization’s system or data deleted from the central controller (e.g., unit number, identity code)?

OTHER

Do you have any concerns about the security of your voice communications? If so, please explain.

Do you have any concerns about the security of your data communications? If so, please explain.

Have there been any incidents concerning the confidentiality, availability, or integrity of your voice or data systems? If so, please explain.

Please provide information on any other issues or concerns that you have concerning voice and data system security.

GLOSSARY

Access Control

A technique used to define or restrict the rights or capabilities of individuals or application programs to communicate with other individuals or application programs and/or to obtain data from, or place data onto, a storage device.

Audit Trail

A chronological record of system activities that is sufficient to reconstruct and review the sequence of events surrounding or leading up to all transactions and actions performed on or by the system.

Authentication

The process of verifying the identity of a user, terminal, or application program to prevent fraud, abuse, and misuse of services.

Automated Information System

A collection of hardware, software, and firmware configured to collect, communicate, compute, disseminate, and/or control data.

Availability

The accessibility and usability of service upon demand by an authorized entity.

Communications Security

Protection measures to protect data that is transferred using communication lines. This includes ensuring that transactions are not invalid, incomplete, or altered.

Computer Room

A facility that houses computer equipment used to store, process, and transmit data (e.g., network servers, workstations, consoles, mainframes, routers).

Confidentiality

The protection which ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration Management

The process of controlling modifications to systems, applications, or to system documentation. Configuration management protects the system or applications against unintended and unauthorized modifications.

Contingency Plan

A plan of action to restore the system's critical functions in case normal processing is unavailable for reasons such as natural disasters, equipment failure, or malicious destructive actions.

Emission Security

Measures to control decipherable electronic signals unintentionally emitted from an information system and communications equipment.

Encryption

The process of transforming plain text into unintelligible form by means of a cryptographic system.

Identification

A code, user name, cards or token that identifies an individual.

Integrity

The protection that ensures that data has not been altered (modified, inserted, or deleted), repeated, or destroyed in an unauthorized manner, either accidentally or maliciously.

Jamming

The intentional transmission of radio signals in order to interfere with the reception of signals from another transmitter.

Key

When used in the context of encryption, a series of numbers which are used by an encryption algorithm to transform plain text data into encrypted (cipher text) data, and vice versa.

Key Management

The process, policies, procedures, and administration encompassing every stage in the life cycle of a cryptographic key, including generation, distribution, entry, use, storage, destruction, and archiving.

Land Mobile Radio

A mobile communications service between land mobile stations or between land mobile stations and base stations.

Mobile Data Terminal

Radio unit installed in a vehicle that provides access to remote database files and communications with the dispatch office.

Over-the-Air-Rekeying (OTAR)

Distribution of cryptographic keys over the air. A central facility, called a Key Management Facility (KMF), stores all keys of use in a system. The KMF distributes the keys by first encrypting the key and then transmitting it over the air to subscriber units in the system. Subscribers decrypt the keys and store them for use among themselves.

Password

A protected word, phrase, or a string of characters that is used to authenticate the identity of a user.

Security Plan

A document which depicts a site’s plan for securing its system.

Virus

A self-executing program that is hidden from view and that secretly makes copies of itself in such a way as to "infect" parts of the operating system and/or application programs.

Vulnerability

A weakness in a system's design or procedure that could be exploited by a threat to gain unauthorized access to a system or impact the system’s availability.